North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Regional

National

International

Banking and Finance Industry

Chemical and Hazardous Materials Sector

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

Government Sector (including Schools and Universities)

Information Technology and Telecommunications

National Monuments and Icons

Postal and Shipping

Public Health

Transportation

Water and Dams

North Dakota Homeland Security Contacts

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **MN farmers affected by floods urged to check grain.** Officials are reminding southern Minnesota farmers and farm businesses to carefully assess the condition of their grain. The state agriculture department said grain may be considered adulterated if any part of the plant used for feed or food — such as corn ears or soybean pods — came into contact with contaminated floodwater. That grain should not be used for human or animal consumption. The agriculture commissioner said the risk of contamination is generally considered highest for crops that were submerged in water that overflowed from rivers or streams. Standing grain that has been in contact with contaminated floodwater from a river or stream should not be blended with uncontaminated grain. Source: http://wcco.com/wireapnewsmn/Minn.farmers.in.2.1952734.html

(Minnesota) **Fire department says chemical spill is contained.** A chemical used to line sewer systems spilled October 6 in St. Cloud, Minnesota, but crews have contained it and say it is not hazardous. The St. Cloud Fire Department's Hazardous Materials Team was called at 4:08 a.m. to Montrose Road and Lancewood Drive. A trailer of styrene monomer spilled, the battalion chief said. Crews put sand around the chemical to contain it. Firefighters were on the scene waiting for a cleanup crew to arrive and remove the chemical. Source: http://www.sctimes.com/article/20101006/NEWS01/110060053/1009/Fire-department-says-chemical-spill-is-contained

(Minnesota) **Chemical incident triggers evacuation at Andover water treatment plant.** Employees at the water treatment plant in Andover, Minnesota, were forced to evacuate October 4 after an unintended chemical reaction. Andover's fire chief said an outside contractor was delivering chemicals to the plant and accidentally poured flourine in the tank that holds chlorine, triggering a reaction that set off hazardous fumes. Emergency response crews and an ambulance were dispatched to the scene at 1815 Crosstown Boulevard around 11:45 p.m. That contractor was treated on the scene, and it was determined he did not need to be transported to the hospital. All of the city's water towers were full at the time, so none of the chemicals were pumped into Andover's water supply. The building is being ventilated while employees move to pump the chemicals that triggered the reaction from the tank. Officials stressed that the public is not in danger. Source: http://www.kare11.com/news/news_article.aspx?storyid=875843&catid=396

National

Feds had alerted state and local authorities to Europe threat. A DHS official said October 4 a bulletin went out 1 day earlier to state and local law enforcement agencies advising them that the U.S. State

Department travel alert in Europe was issued based on intelligence they had already been made aware of. The four-page bulletin, a copy of which was obtained by CNN, is titled "Al Qaeda Threat to Europe." It said it was issued "to raise general security awareness and as part of our ongoing effort to provide information about any potential terrorist threat against the United States or our allies in Europe." DHS also is briefing representatives from the private sector, including hotels and commercial properties, regarding the threat environment. The DHS official said that the Transportation Security Administration continuously deploys threat-based security measures as a result of intelligence. Source: http://articles.cnn.com/2010-10-04/us/terrorist.threat.security_1_homeland-security-law-enforcement-al-qaeda-threat?_s=PM:US

More than half of critical infrastructure firms have been hit by state-sponsored attacks. Politically motivated, state-sponsored attacks are happening regularly: Fifty-three percent of critical infrastructure firms around the globe said they have been hit with an attack aimed at a specific political goal, a new report from Symantec found. A survey of 1,580 energy, banking and finance, healthcare, IT, emergency services, and communications firms worldwide found that these firms have each suffered about 10 such politically motivated, state-sponsored attacks in the past 5 years. Around 60 percent of these attacks worldwide were somewhat to extremely effective, the respondents said, and 74 to 77 percent of the firms in North America said the attacks on them were "effective." Small businesses suffered the most bruising attacks, according to the report, with an average cost of $850,000 per attack. Worries about these targeted attacks are high of late, with the Stuxnet worm attack that went after factory floor plant systems. Stuxnet serves as a cautionary tale of the potential of these brands of attacks, according to Symantec. The Symantec 2010 Critical Infrastructure Protection Study, which was conducted by Applied Research, found that 48 percent of these firms expect more such attacks in the next year, and 80 percent said these attacks will either remain constant or will increase. Source: http://www.darkreading.com/security_monitoring/security/attacks/showArticle.jhtml?articleID=227600086&subSection=Attacks/breaches

INTERNATIONAL

Euro terror alert spotlights voiceprint technology. Did their voices betray them? The discovery of an alleged terror plot against Europe owes at least some of its success to "voiceprint" technology that allows law enforcement to electronically match a voice to its owner. The technique — which some compare to fingerprinting — can be a powerful anti-terror tool, officials increasingly believe. Law enforcement agencies are already considering how a voice database could help thwart future plots. The reported plot against European cities, in which suspects allegedly spoke of a Mumbai-style shooting spree, has triggered travel warnings and refocused attention on al-Qaida activities on the Pakistan-Afghanistan border, where several of the voices were recorded. The British eavesdropping agency GCHQ deployed voice identification software to help uncover the plot officials say has targeted Germany, Britain, and France — with famed sites such as Notre Dame Cathedral and the Eiffel Tower under close surveillance. Despite progress made in quashing the plot, officials still speak of an ongoing threat. Police in southern France October 5 arrested 12 suspects in sweeps against suspected Islamic militant networks, including three men linked to a network recruiting fighters for Afghanistan. Source: http://www.google.com/hostednews/ap/article/ALeqM5isVrwHYielnHBYr4EvvWIzuJ8I0gD9ILMII02?docId=D9ILMII02

Insecurity in Sanaa as Westerners targeted once again. The small number of diplomats, consultants, aid agency staff and energy sector employees based in Yemen's capital, Sanaa, are growing used to increasing restrictions on their personal freedom, which tighten after every security scare. The October 6 attacks come 6 months after the outgoing British ambassador was targeted in a failed assassination attempt. The new British ambassador is due to take up his post within weeks. Two "near-miss" attacks in 6 months will raise questions about the role the British are playing in Yemen, and why British diplomats are repeatedly being targeted by al-Qaeda-style groups. On a practical level, the British embassy — which sits directly on a main road, opposite the landmark Movenpick Hotel — is currently more accessible than the U.S. embassy. Trucks and cars roar past the gates of the British embassy on a busy dual carriageway, while the U.S. embassy is now cordoned off to passing traffic and all visiting vehicles require advance security clearance to enter the American cordon. Similarly, the U.S. ambassador lives inside his embassy compound, while the U.K. ambassador has to commute across town every day to reach the office. There is simply more opportunity to strike high-profile British targets. Policemen stopped cars near the British embassy after the rocket attack. British military trainers have been working closely with the Yemeni government for several years, supporting both the coastguard and the counter-terrorism unit. American military trainers and planners are playing a more significant role, which includes sharing intelligence and conducting secret joint operations with the Yemeni military. Source: http://www.bbc.co.uk/news/world-middle-east-11485774

Extremists warn of biological strike in India. An extremist entity indicated it would carry out a biological strike on the Indian state of Assam if its backers were not released within 24 hours, Iran's Islamic Republic News Agency reported October 3. "Free all our Jihadi brothers who are in Central Jail, Guwahati, stop all activities against Jihad in Assam, stop all project of develop (sic) in Assam," said the e-mail, sent to a Guwahati-based television station by a group calling itself "Indian Mujahideen (Assam)." "For your kind information, biological war contain all disease that make death to all and biological weapon too," said the document, signed by the organization's self-described head of marketing. Local authorities were attempting to identify the Internet Protocol address from which the e-mail message was sent. "We are taking the matter seriously and already experts are on the job to ascertain from where the e-mail originated and also about the credentials of the group on whose banner the mail was sent," the inspector General of Assam Police said. "We really don't know or heard about any such outfit named Indian Mujahideen (Assam). But then we shall surely investigate," a second law enforcement official added. Source: http://www.globalsecuritynewswire.org/gsn/nw_20101004_1995.php

IRA dissident car bomb hits Londonderry businesses. A dissident Irish Republican Army car bomb damaged a hotel, bank and other businesses but caused no injuries October 5 in the Northern Ireland city of Londonderry, the sixth such attack this year in the British territory. Analysts said the middle-of-the-night blast — which blew out window frames and glass in several buildings, doing particular damage to the bank — appeared to have been timed to undermine the city's major Sinn Fein politician.The Real IRA splinter group later claimed responsibility for the attack in a coded telephone call to the news desk of a city newspaper, the Derry Journal. The dissidents telephoned warnings to local businesses, giving the police about 1 hour to evacuate the area — including a nursing home — before the explosion. "I don't know what these people are trying to achieve," the city mayor said of the dissidents, who operate from Londonderry's working-class Catholic districts. "This city will not be

defeated by a minority of people who think they'll free Ireland by bombing hotels." Analysts said the Real IRA may have targeted the hotel, in part, because it is hosting a meeting later this week between local politicians and police officers in Londonderry, a predominantly Catholic city. Source: http://www.google.com/hostednews/ap/article/ALeqM5gKL1X_QCDc7zPJD-6BhBHaSdlz7gD9ILIJE00?docId=D9ILIJE00

Russia wheat production may drop 33%, USDA unit says. Russia's wheat production may plunge by 33 percent this year after the most-severe drought in 50 years harmed crops, a U.S. Department of Agriculture (USDA) unit said. Output will fall to 41.5 million metric tons in the year that began July 1 from 61.7 million tons last year, the USDA's Foreign Agricultural Service (FAS) said in a report posted on its Web site October 4. The attache's estimate was below the official U.S. projection announced in September. Russian exports will plunge 78 percent to 4.1 million tons, the FAS said. "Significant grain area was destroyed by drought, and harvested area might be one of the lowest in the last 10 years." Russia, once the world's third-largest grower, barred exports of grains in August. On September 10, the USDA projected that Russia would produce 42.5 million tons of wheat and export 3.5 million tons. Russian barley output may drop 54 percent to 8.2 million tons from 1 year earlier, and exports may plummet 91 percent to 250,000 tons, the U.S. attache said. Corn production may drop 11 percent to 3.5 million tons. Wheat prices fell in Chicago October 4, capping the longest slump in 4 months, as rains in Russia and Eastern Europe improved the prospects for winter crops. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2010/10/04/bloomberg1376-L9S51X6JTSEK01-5BJKULM0N9V0B7ICKEEL11FSA2.DTL

Banking and Finance Industry

'Man In the mobile' attacks highlight weaknesses in out-of-band authentication. Recent attacks that use the increasingly popular Zeus Trojan are demonstrating that widely used methods of out-of-band authentication might be flawed, experts said. New attack techniques dubbed "Man in the Mobile" (MitMo) are allowing black hats to leverage malware placed on mobile devices to get around password verification systems that send codes via SMS text messages to users' phones for confirmation of identity. "In a transaction verification system, the customer receives a text message with the transaction details and a code to enter back into the Web site — only if the transaction details match the real transaction," explained the CEO of Trusteer. "Transaction verification was considered a good solution to protect against [MitMo] attacks, where malware attempts to submit a transaction on behalf of the victim. The expansion of Zeus' capabilities to carry out MitMo attacks is yet another step in the cat-and-mouse game that banking security professionals continue to play with hackers to ensure users are who they say they are. Banks need to find ways to educate users and help them secure their channels of authentication, the CEO said. Source: http://www.darkreading.com/authentication/security/client/showArticle.jhtml?articleID=227700141

Massive iTunes phishing attack. Apple's popular iTunes platform has become a major target for hackers looking to steal credit card data from the service's millions of users. Victims receive a cleverly-crafted e-mail informing them they have made an expensive purchase on iTunes. The user, having never made the purchase to begin with, is concerned by the e-mail and naturally tries to resolve the problem –- in this case by clicking on the proffered (fake) link. After clicking the link, the victim is asked to download a fake PDF reader. Once installation is complete, the user is redirected to an infected Web page containing the ZeuS Trojan, which is specifically designed to steal personal

data. This phishing attack was uncovered shortly after a similar phishing attack targeting LinkedIn users appeared last week, which appears to have originated in Russia. This technique has been reported to the Anti-Phishing Working Group, which has started to block some of the Web addresses linked to in the fake e-mail. PandaLabs advised all users to be wary of any e-mails related to iTunes, regardless of how genuine they seem. Users who think they may have been affected are urged to scan their computers thoroughly to locate and remove any possible threats. Source: http://www.net-security.org/secworld.php?id=9945

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(California) **Monterey hotel evacuated after bomb scare.** Guests at the Travel Lodge and the Econo Lodge hotels in Monterey, California, were evacuated October 5 after police found a U.S. World War II pineapple type hand grenade in a man's car in the parking lot of the Travelodge. Police found a man sleeping in his vehicle, and, after searching the vehicle, found various narcotics, narcotics paraphernalia, a forged prescription, a billy club, and the hand grenade. The Monterey County Sheriff's Department Bomb Squad responded to the scene and transported the item from the scene for later destruction. The parking lot was evacuated and guests were relocated to rooms away from that area of the parking lot. The vehicle was towed from the scene and the parking lot was re-opened to the public at about 4:30 a.m. Source: http://www.kionrightnow.com/Global/story.asp?S=13269566

(Oregon) **IED discovered on the North Spit sand dunes.** According to the Coos County Sheriff's Department, a Charleston, Oregon man discovered an Improvised Explosive Device (IED) perched on a small sand dune at North Spit in North Bend, Oregon, at 11 a.m October 2. A Deputy sheriff located the device and determined it to be a possible IED. A call was made to the Oregon State Police Bomb Squad, based in Central Point, who responded to the area just before 5 p.m. The device was rendered harmless in a matter of minutes. Upon further investigation, the bomb technicians described the device as a viable IED. They said had it been tampered with, it could have caused serious physical injury to the person holding it or standing nearby. The device's construction will not be released as the investigation is ongoing. Source: http://www.kcby.com/news/local/104280414.html

(Arizona) **Police shut down Phoenix street to investigate suspicious package.** A downtown Phoenix street was shut down and surrounding businesses evacuated for several hours October 4 as police investigated a suspicious package found on Van Buren Street. Officials said the box raised suspicions after it was discovered to have some type of wires coming from inside. A bomb squad unit at the scene investigated and detonated the device. The box was reportedly found in an alleyway behind Valley Metro headquarters. Phoenix police confirm they are looking into the possibility the scare may be connected to a current transit dispute. Source: http://www.abc15.com/dpp/news/region_phoenix_metro/central_phoenix/police-shut-down-phoenix-street-to-investigate-suspicious-package

Communications Sector

Data overload block tracking of sex offenders. A company that provides electronic monitoring to track sex offenders, parolees and others said its system shut down after unexpectedly hitting its data storage limit, leaving authorities across 49 states unaware of offenders' movement for 12 hours. Prisons and other corrections agencies were blocked from getting notifications on about 16,000 people being tracked,a BI Incorporated spokesman said. The system operated by the Boulder, Colorado-based company reached its data threshold — more than 2 billion records — October 5. Tracking devices continued to record movement October 5, but corrections agencies could not immediately view the data. The company has substantially increased its data storage capacity and has not heard of any safety issues, the spokesman said. People being monitored were unaware of any problems. BI contracts with about 900 government agencies across the country for monitoring and notification services, including real-time monitoring and delayed notifications about offender whereabouts. The agencies vary widely, and include state prison systems, sheriff's departments, and pre-trial service entities, the spokesman said. Before the shutdown, the company's database could hold 2.1 billion records, such as a GPS address or an alcohol reading, the spokesman said. The company spent October 5 expanding the threshold to more than 1 trillion records. The spokesman said staff will work to develop a system that can supply early warnings as the database fills. Source: http://www.google.com/hostednews/ap/article/ALeqM5grcUbAX19wQmbvjFli763EYn1ohgD9IMN93O0?docId=D9IMN93O0

The growing security risk of fiber tapping. Corporate data centers, with their vast stores of business-sensitive information, present a tempting target for criminal groups. But today's enterprise security systems are so sophisticated that hacking into an enterprise data center is nearly impossible. But what if there were another way to get at this valuable data that circumvented most traditional security software? Welcome to the shady world of fiber tapping, where instead of physically accessing a site or attempting to hack into it, the cyber criminal simply taps the optical fiber leading up to it. Cases of fiber tapping are relatively rare, but with the cost of fiber tapping devices falling and the number of enterprises storing sensitive data in remote datacenters growing in tandem with the rise of cloud computing, many more are likely in the future. Source: http://www.v3.co.uk/computing/analysis/2270985/growing-security-risk-fibre

(Maine) **Man charged with sabotaging phone service.** A Saco, Maine, man faces felony charges of aggravated criminal mischief after police accused him of intentionally unplugging telephone and Internet connection equipment at his former employer, GWI. The 40-year-old suspect used his employee access badge September 11 to enter GWI's Jefferson Street facility in Biddeford where he unplugged circuitry, police said. The resulting disruption shut down telephone service to 700 residents and 50 businesses including the Biddeford Police Department. It also disrupted Internet service for about 1,000 customers. An employee of GWI for 8 years, the suspect resigned, then tried to rescind that resignation. The company refused to allow him to take it back and shortly afterward he broke into the facility. Source: http://www.kjonline.com/news/Saco-Maine-man-GWI-sabotage-phone-service-Sept-11.html

Critical Manufacturing

Cadillac SRXs recalled due to fire hazard. Cadillac SRX crossovers from the 2010 model are being recalled due to damage in the power steering line, General Motors (GM) and the National Highway Traffic Safety Administration announced on October 7. GM said they will be recalling around 4,000 of the 2010 Cadillac luxury SUV crossovers. If the line is damaged, it could potentially pose a fire hazard as power steering fluid may leak, according to a news release from the company. The fluid could drip or spray onto heated engine parts, which in turn could cause a fire. GM said there has only been one reported fire related to the power steering problem. Most of the recalled vehicles are located in the United States, and 341 were exported to China. All of the vehicles were built last December. GM said that Cadillac dealers will replace the power steering fluid line. Source: http://www.theepochtimes.com/n2/content/view/43847/

FAA modifies restrictions for new Boeing jets. A week after issuing interim rules to protect aircraft from the wake turbulence generated by Boeing's latest jetliner models, federal regulators reversed course and said the restrictions were premature. The Federal Aviation Administration's (FAA) surprise move October 5 left industry officials and safety experts uncertain about the potential hazards of flying closely behind the 787 Dreamliner and the larger 747-8, both of which are currently undergoing flight tests. The situation was further confused when an FAA spokeswoman said the interim rules contained "some mistakes." The interim rules, would have required aircraft to remain at least 10 miles behind the new Boeing jets during a large portion of the descent towards the airport. Such spacing and other restrictions — especially around busy hub airports — could frustrate airlines such as All Nippon Airways, Japan Airlines Corp. and Cargolux Airlines International S.A. that are among the first slated to put the Boeing models into service. Source: http://online.wsj.com/article/SB10001424052748703843804575535191275956762.html?mod=googlenews_wsj

Defense/ Industry Base Sector

U.S. GAO: National Nuclear Security Administration needs to ensure continued availability of Tritium for the weapons stockpile. The National Nuclear Security Administration (NNSA) has been unable to overcome technical challenges it has experienced producing tritium. To produce tritium, stainless steel rods containing lithium aluminate and zirconium — called tritium-producing burnable absorber rods (TPBAR) — are irradiated in the Tennessee Valley Authority's (TVA) Watts Bar 1 commercial nuclear power reactor. Despite redesigns of several components within the TPBARS, tritium is still leakingv—vor "permeating"v—vout of the TPBARs into the reactor's coolant water at higher-than-expected rates. NNSA has not been producing as much tritium as it planned. NNSA and TVA officials are continuing to develop plans to increase the number of TPBARs that will be irradiated, as well as, if necessary, the number of reactors participating in the program. NNSA officials said they will be able to meet future requirements through a combination of harvesting tritium obtained from dismantled nuclear warheads and irradiating TPBARs. Source: http://www.gao.gov/products/GAO-11-100

Remington upgrading M24 sniper rifle. The M24 sniper rifle is getting a host of upgrades, including a new caliber that will increase a sniper's effective range by 50 percent. The $28 million contract, announced September 20, requires manufacturer Remington to upgrade 3,600 rifles over 5 years. The resulting M24E1 will transition from the 7.62mm NATO caliber (.308 Winchester) to a .300 Winchester Magnum. The change is expected to expand a sniper's effective range from 800 to 1,200 meters. The upgrades are largely the result of snipers in Afghanistan calling for a rifle that provides more power and longer range. The requirement was captured in an Operational Needs Statement from 10th Mountain Division in March 2006. Source: http://www.militarytimes.com/news/2010/10/army-remington-upgrades-m24-sniper-rifle-100410w/

Emergency Services

EMTs question readiness for WMD strike. Only 15 percent of emergency medical technicians in a recent survey said they were highly confident of their employer's ability to deal with the aftermath of a weapons of mass destruction (WMD) strike, EHS Today magazine reported. The nationwide survey conducted by Meridian Medical Technologies Inc. found that one quarter of interviewed medical first responders said either their department offered no training in responding to a WMD attack or had reduced the quantity of time spent preparing for such an event. However, 37 percent said they had seen a boost in training time in the last 5 years. Just 42 percent of emergency medical technicians said their agency is given recurring instruction on handling an attack involving terrorists and chemical, biological, radiological, nuclear or explosive weapons. In excess of 25 percent of those surveyed said their medical vehicles were not outfitted with individualized protective gear and the medical countermeasures that would be required following a WMD attack with high casualties. For those ambulances that do have CBRNE medications, 86 percent of responders said there are too few to be used on the public. Source: http://www.globalsecuritynewswire.org/gsn/nw_20101005_2880.php

(Florida) **White powder found at jax beach police HQ.** A suspicious package was found October 4 at the Jacksonville Beach, Florida Police Department and a hazardous materials team is trying to determine what it contained. Police said that employees found a small container containing a white powder near the pass-through window to the records section at the police station on Penman Road. No symptoms were reported and the container was safely reopened. The police do not know when it was put there or who did it, but they are investigating. Source: http://www.news4jax.com/news/25272330/detail.html

Energy

440 million new hackable smart grid points. By the end of 2015, the potential security risks to the smart grid will reach 440 million new hackable points. SmartPlanet interviewed Lockheed Martin's general manager of Energy and Cyber Services. "By the end of 2015 we will have 440 million new hackable points on the grid...Every smart meter is going to be a hackable point. There are devices and routers in all of the substations that are hackable. Automated devices at home all become hackable points. We're making the whole network from generation to distribution and meter fully automated, so that's hackable. If you can communicate with it, you can hack it," he stated. Source: http://blogs.computerworld.com/17120/400_million_new_hackable_smart_grid_points

(Pennsylvania) **Copper heist caused outage, police say.** More than 300 Penelec customers in the Wood and Robertsdale areas of Huntingdon County, Pennsylvania lost power October 3 into October 4 after vandals knocked down power lines and stripped away about 1,000 feet of copper wiring, authorities said. The suspected crime occurred about 1 mile south of Route 913 in Wood Township when an unknown suspect cut down trees through a heavily wooded area, causing the wires to fall to the ground, and then a cutting instrument was used to cut into the wires, state police at Huntingdon said. Five spans of primary wires — a span covering from pole to pole — were taken down in the incident. Source: http://www.altoonamirror.com/page/content.detail/id/542967/Copper-heist-caused-outage--police-say.html?nav=742

Food and Agriculture

(Ohio) **Valley Farm Meats recalls products for possible Listeria.** Valley Farm Meats of Strasburg, Ohio, announced a voluntary recall of approximately 1,187 pounds of various ready-to-eat meat items that may be contaminated with Listeria monocytogenes. The products subject to recall include: Trail Bologna or Prepared for Abel's Cheese Trail Bologna (612 pounds); Smoked Snack Sticks (125 pounds); and Smoked Sliced Bacon (450 pounds). The problem was discovered as a result of a routine sample collected by the Ohio Department of Agriculture's Division of Meat Inspection and analyzed by the department's consumer analytical lab. The department has not received reports of illnesses associated with consumption of this product. Source: http://www.usagnet.com/state_headlines/state_story.php?tble=OH2010&ID=847

(Iowa) **Dam failure may hurt river's fish stock.** A fish expert is raising concerns about the future of what had been a world-class, smallmouth bass fishery in a silt-filled river below the failed Lake Delhi dam in Iowa. Iowa Department of Natural Resources officials found adult smallmouth bass in the cloudy Maquoketa River while sampling fish stocks October 4. The concern for the next 5 years is how the fish will reproduce and sustain themselves now that a 6-inch layer of muck covers the rocky stream bed, which was ideal for spawning areas, a fisheries biologist said. The dam failed July 24, draining a 9-mile-long recreational area. After more tests October 6, the biologist will compare data to quantify the aftermath of the dam breach on fish stocks. Source: http://www.desmoinesregister.com/article/20101006/NEWS/101005022/1001/NEWS/Dam-failure-may-hurt-river-s-fish-stock

Government Sector (including Schools and Universities)

FBI program to boost security at bases. Nearly a year after a shooting rampage at Fort Hood, Texas, the Pentagon is taking new steps to beef up security and surveillance programs at its bases, and will join an FBI intelligence-sharing program aimed at identifying future terror threats, U.S. officials said. The new partnership with the FBI's eGuardian program comes 2 years after the Pentagon shut down a controversial anti-terror database that collected reports of suspicious activity near military installations. The now-defunct program, called TALON, was closed after revelations it had improperly stored information on peace activists. Defense officials have moved carefully to set up the new programs, trying to balance the protection of the nation's armed forces with the privacy and civil rights of Americans. Source: http://www.military.com/news/article/fbi-program-to-boost-security-at-bases.html?ESRC=topstories.RSS

(New Hampshire) **Bomb scare: Suitcase causes evacuation of Portsmouth federal building.** A report of a suspicious suitcase left on Penhallow Street in Portsmouth, New Hampshire prompted the evacuation of the federal building October 6 before a New Hampshire State Police bomb squad blew up the piece of luggage determining it posed no threat. Shortly after 6 p.m., a charged water cannon was used to blow open a case that was later determined to have contained a laptop computer and business cards that ended up littering the street. The bomb squad commander said the suitcase never posed a threat, but he said employees at the Thomas J. McIntyre Federal Building were justified in notifying officials. Portsmouth officers were summoned to the building at 80 Daniel Street at 3:58 p.m. when officers with the Federal Protective Service located the suspicious briefcase outside the entrance. Source: http://www.fosters.com/apps/pbcs.dll/article?AID=/20101007/GJNEWS_01/710079663/-1/FOSNEWS

Terror infiltration addressed in Army reg. A new Army Regulation, 381–12, Military Intelligence Threat Awareness and Reporting Program, provides new "policy and responsibilities for threat awareness and education and establishes a requirement for Department of Army (DA) personnel to report any incident of known or suspected espionage, international terrorism, sabotage, subversion, theft, or diversion of military technology, information systems intrusions, and unauthorized disclosure of classified information." According to the new regulation, "the Army is a prime target for foreign intelligence and international terrorist elements" and "faces the threat of espionage, sabotage, subversion, and international terrorism from within and OCONUS." "The Army also faces threats from persons on the inside (the insider threat), those with placement and access in an organization who may compromise the ability of the organization to accomplish its mission through espionage, acts of terrorism, support to international terrorist organizations, or unauthorized release or disclosure of classified or sensitive information," the regulation announcement stated, adding "the potential of the insider threat to cause serious damage to national security underscores the necessity for a focused and effective TARP (threat awareness reporting program)." The new regulation provides guidance on detection of behavior that may be exhibited by a person engaged in espionage, indicators of insider threats of terrorism, and signs of extremist activity that may pose a threat to U.S. military facilities or operations, and added "the Director, Army G-2X as the primary staff element responsible for establishing and maintaining a centralized system of control for the reporting of threat incidents and follow-on counterintelligence investigations." Source: http://www.hstoday.us/content/view/14994/149/

(Illinois) **2 schools evacuated after explosives found nearby.** Chicago police bomb and arson officers detonated commercial-grade explosives along railroad tracks in a West Englewood, Illinois, neighborhood October 4, police said. The discovery of the explosives forced the evacuation of two schools, said a Chicago police spokesman. The explosives were found about noon near the CSX railroad tracks near 73rd Street and Hoyne Avenue, he said. Police officials said the explosives were commercial grade which were dumped near the tracks. At 3:45 p.m. officials with the bomb and arson unit detonated the explosives and issued an all-clear, indicating that there was no further threat, the spokesman said. As a precaution, officials evacuated the South Side Occupational Academy high school and the Randolph Elementary School. Police said they are investigating how the explosives got to the site. Source: http://www.chicagobreakingnews.com/2010/10/2-schools-evacuated-after-suspicious-package-found-nearby.html

Information Technology and Telecommunications

Cryptome hacked, founder e-mail account ransacked. Cryptome.org, the well-known whisteblowing site, was hacked the weekend of October 2 and 3, and all of its content (approximately 7GB of data) was deleted by the hacker who then left a message on the defaced home page. The hacker, who goes by the handle "RuxPin," has supposedly contacted Wired.com and said that two other members of the hacking group Kryogeniks were actually responsible for the breach. They supposedly managed to steal the password for one of the e-mail accounts belonging to the site's founder nearly 1 month ago, when the system that stored the passwords was breached. Having the password for the e-mail account that was listed as the contact address for the site, they simply used it to ask for a reset of the password for Cryptome's hosting account. The site founder is not worried about rummaging or the deleting of the content, since it is open source and they have backup. What he is really worried about is the fact that, along with the content, the hackers managed to download a repository of e-mail correspondence between him and his sources (some reputed to be WikiLeaks insiders) - who, in theory, can be revealed by tracking the e-mail addresses. Source: http://net-security.org/secworld.php?id=9954

The rise of crimeware. Nearly 2 billion people today use the Internet and in doing so, expose themselves to an extensive and growing number of malware threats. CA researchers identified more than 400 new families of threats, led by rogue security software, downloaders and backdoors. Trojans were found to be the most prevalent category of new threats, accounting for 73 percent of total threat infections reported around the world. Importantly, 96 percent of Trojans found were components of an emerging underground trend towards organized cybercrime, or "Crimeware-as-a-Service." The most notable threats and trends of 2010 to-date include: Rogue or fake security software, also known as scareware or Fake AV, the first half of 2010 saw this category of malware continue its dominance. Google became the preferred target for distribution of rogue security software through Blackhat SEO, which manipulates search results to favor links to infected Web sites domains. Some 96 percent of Trojans detected in H1 2010 functions as a component of a larger underground market-based mechanism which CA has termed "Crimeware-as-a-Service." Research revealed cybercriminals' growing reliance on using cloud-based Web services and applications to distribute their software. Source: http://www.net-security.org/malware_news.php?id=1488

FCC may confront ISPs on Bot, Malware scourge. The Federal Communications Commissions (FCC) may soon kickstart a number of new initiatives to encourage Internet service providers (ISPs) to clean up bot-infected PCs and malicious Web sites on their networks, KrebsOnSecurity has learned. Earlier this year, the FCC requested public comment on its "Cybersecurity Roadmap," an ambitious plan to identify dangerous vulnerabilities in the Internet infrastructure, as well as threats to consumers, businesses and governments slated for release in January 2011. The associate bureau chief of the FCC's Public Safety & Homeland Security Bureau said there are several things the commission can do to create incentives for ISPs to act more vigorously to protect residential users from infections by bot programs. Source: http://krebsonsecurity.com/2010/10/fcc-may-confront-isps-on-bot-malware-scourge/

HTML attachment spam exploded in recent months. Spam campaigns, which generate e-mails with malicious HTML attachments, have been particularly aggressive during the past 5 months and they

accounted for between 2 and 8 percent of all spam. According to data from security vendor Sophos, the most affected months were June and September, when the volume of spam with HTML attachment reached 8 percent of the total junk-mail traffic. In comparison, the months of July, August and October have seen average distribution levels of 2 percent to 3 percent, which is still significant. The majority of rogue HTML files served in this manner consist of phishing pages or contain JavaScript code that redirects users to malware pushing Web sites. As far as phishing is concerned, attacks employing this technique have targeted the customers of organizations like PayPal or Banchi de Credito Cooperativo. "Instead of setting up a bogus financial website, scammers insert the phishing contents directly into the HTML attachment," the Sophos researchers explain. The JavaScript redirect method is much more common, and the second half of September has seen waves of e-mails with random subjects, content, and attachment names. Source: http://news.softpedia.com/news/HTML-Attachment-Spam-Exploded-in-Recent-Months-159367.shtml

Fake browser warnings dupe users into downloading 'scareware'. Scammers are spoofing the anti-malware warnings of popular browsers to dupe Windows users into downloading fake security software, Symantec said October 4. Several malicious Web sites are displaying phony versions of the alerts that Google's Chrome and Mozilla's Firefox present when users encounter pages suspected of hosting attack code, said a Symantec researcher in a post to the firm's blog. Rather than simply warn users that the page they are about to visit may be dangerous — as do the legitimate alerts — the sham versions also include a prominent message that suggests downloading a browser security update. In reality, no browser offers its users security updates from its anti-malware warning screen. Anyone who accepts the update actually downloads bogus software, often called "scareware" because it bombards users with endless fictitious infection warnings until people pay $40 to $50 to buy the useless program. Even the cautious can be nailed by these sites. Users who refuse the mock updates are assaulted by a multi-exploit toolkit that includes attack code for 10 different vulnerabilities in Windows, Adobe Reader, Internet Explorer and Java. Windows PCs that have been kept up-to-date with bug patches will be immune from the exploit kit, however. Source: http://www.computerworld.com/s/article/9189399/Fake_browser_warnings_dupe_users_into_downloading_scareware_

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

(California) **Leaking package forces evacuation of state office.** A package that was leaking formaldehyde is being blamed for forcing the evacuation of a state department of fish and game office in Sacramento, California. A spokesman for the Sacramento Fire Department said a hazmat team was sent to the office around 11:34 a.m. October 7 when several employees said they were having difficulty breathing after coming in contact with a package that had just been delivered by Federal Express. A fire spokesman said two employees were taken to a hospital, though their symptoms were not considered serious. About 20 minutes later, firefighters with the Sacramento Metropolitan Fire District were called to a business several miles away in suburban North Highlands, where employees were complaining of similar symptoms. Fire officials determined that a separate

package had leaked onto the two packages at a distribution center. Source: http://www.sacbee.com/2010/10/07/3088766/leaking-package-forces-evacuation.html

(Illinois) **Suspicious mail closes down Busse Highway.** Officials are still trying to determine what the substance was in a suspicious piece of mail that forced the closure of Busse Highway in Park Ridge, Illinois, October 4. The suspicious envelope was delivered to a business in the 600 block of Busse, police said. According to a police spokesman, the woman who discovered the envelope while opening mail is not showing any signs of illness. "The person that handled the mail is experiencing nothing," he said. "We treat it with the utmost respect and care," the spokesman said of the hazardous materials response. "We go into it with all the precautions for the personnel." As of 2 p.m., about 10 to 15 pieces of fire equipment and hazardous material specialists were on the scene. The road was closed from Western to Seminary avenues, although businesses and homes in the area were not all evacuated. Source: http://www.journal-topics.com/pr/10/pr101004.1.html

PUBLIC HEALTH

Doctor shortage looming? Use nurses, U.S. report says. Nurses can handle much of the strain that healthcare reform will place on doctors and should be given both the education and the authority to take on more medical duties, the U.S. Institute of Medicine said October 5. A report from the institute calls for an overhaul in the responsibility and training of nurses and said doing so is key to improving the fragmented and expensive U.S. healthcare system. "We are re-creating nursing in America," the president and CEO of the nonprofit Robert Wood Johnson Foundation said at a news conference. "We believe that this report and the implementation of its findings is vital to the strength of healthcare in this nation," she said. Nurses already often deliver babies, counsel patients with heart disease or diabetes, and care for dying cancer patients — and these roles should be expanded nationally and paid for by both public and private insurers, the report said. The U.S. healthcare reform law passed in March is expected to add 32 million Americans to health insurance company rolls. Several groups, including the Institute of Medicine, have forecast shortages of doctors to provide care. Last month, the Association of American Medical Colleges released new estimates that showed 63,000 more doctors would be needed in 2015 than would be available. Source: http://www.reuters.com/article/idUSN0518768220101005

Biosecurity bill aims to boost international WMD cooperation. A bill introduced by a Democratic Representative from California (HR 6297) would provide U.S. training assistance to other nations while boosting their capabilities to detect and withstand biological outbreaks or attacks. The legislation would direct the U.S. State Department to assess international laws applicable to biosecurity with the goal of strengthening a common legal framework for dealing with biosecurity issues. It also would set up an International Biosecurity Task Force, composed of experts outside of government, to advise the International Biosecurity Initiative. The California Representatives wants to get his legislation attached to The WMD Prevention and Preparedness Act (H.R. 5498), a comprehensive bill intended to boost defenses against weapons of mass destruction (WMD). Section four of H.R. 5498 deals with international issues, calling for international information sharing, an interagency task force on global biosecurity, and the promotion of the Biological and Toxin Weapons Convention (the major international treaty for dealing with biowarfare and bioterrorism concerns). Source: http://www.hstoday.us/content/view/14976/149/

(Virginia) **Possible measles exposure at Reagan National Airport.** People in Reagan National Airport's Terminal C may have been exposed to measles September 23, according to Arlington, Virginia health officials. Someone with the illness was in the terminal between 8:45 a.m. and 12:30 p.m. People at risk for infection who were on the plane have already been notified. Arlington County Public Health officials said they are acting out of an abundance of caution. Most people have been vaccinated for measles, but the agency recommends a doctor be called if one notices any symptoms of the disease, if one is pregnant, or if one has a weakened immune system. Measles is a highly contagious illness that is spread through coughing, sneezing, and contact with secretions from the nose, mouth, and throat of an infected individual. Source: http://wtop.com/?sid=2068359&nid=726

(Massachusetts) **Bomb threat forces medical office evacuation.** A bomb threat sent workers and patients at a medical building in Salem, Massachusetts into the parking lot for about 1 hour October 4. The deputy chief said police did not find anything suspicious inside the medical offices at Stiles Road, where the threat was called in to a pediatrician's office. When Salem police arrived, the building had already been evacuated, he said. The incident is under investigation. The facility's technology director for Salem Radiology, the building's biggest client, said he heard about the bomb scare around 9:15 a.m. October 4, one of the office's busiest times. Source: http://www.eagletribune.com/newhampshire/x537488284/Bomb-threat-forces-medical-office-evacuation

TRANSPORTATION

(Pennsylvania) **Philadelphia flight grounded after unidentified baggage handler vanishes.** An unidentified baggage handler prompted a Bermuda-bound flight out of Philadelphia International Airport to be evacuated October 7. According to police, 102 passengers and five crew members were removed from US Airways Flight 1070 around 11 a.m., after two baggage handlers that were loading the plane noticed that a third baggage handler was in uniform, but was not wearing a security badge. When confronted, the man vanished from the tarmac. After the passengers were deplaned, the aircraft was towed to a secure area of the airport where police removed and checked each piece of luggage with the help of bomb-sniffing dogs. The plane was also checked for explosives, though no hazardous materials were found. The incident is not expected to be terror-related, an FBI spokesperson said. Source: http://news.travel.aol.com/2010/10/07/philadelphia-flight-grounded-after-unidentified-baggage-handler/

Plane Finder AR app heightens security fears. Security experts have lashed out against an airline tracking app, claiming that it could be used by terrorists to shoot down planes using surface-to-air missiles. The Plane Finder AR application for the iPhone and Android OS platform is designed to allow users to see the height, position and speed of an aircraft by pointing their smartphones to the sky. The app also tells them the destination of the aircraft along with departure point and the course it would take. Experts have claimed that the app, which has been developed by UK firm Pinkfroot, could be used by terrorists to shoot down planes or cause mid-air collisions. Pinkfroot has said that it had designed the app to give delayed information that might foil a terrorist attack, if it was to happen. Source: http://www.portal.itproportal.com/portal/news/article/2010/10/4/plane-finder-ar-app-heightens-security-fears/

(New York) **Heightened security at NYC subways.** The New York Police Department's (NYPD) commissioner warned that New York City remains the primary target for terrorists. As rail traffic increases around the upcoming holiday, at Penn Station and throughout the Amtrak system, there is an increased show of force reportedly known as "Operation Railsafe." Officials hope it will bring heightened awareness. "Forty percent of attacks over the last 20 years have been against transit facilities," the commissioner said. While intelligence officials press the hunt for suspected terrorists said to be planning an alleged plot in Europe, the threat of terrorism in New York City is the focus of an NYPD shield conference. They also are training to counter a favorite terrorist tactic aimed at striking first responders with a secondary explosion. The NYPD also continues to pour anti-terrorism resources and highly trained officers into the world's largest mass transit system. Source: http://abclocal.go.com/wabc/story?section=news/local&id=7707788

(Arizona) **Tempe police explode suspicious package.** A large oversized briefcase found at the Veterans Way and College Avenue light-rail stop in Tempe, Arizona October 5, disrupted rail service and caused a street closure. Trains could not pass through the station and buses were used to transport people between adjacent stops at Mill Avenue and Rural Road. Authorities deployed the bomb squad unit, which determined the package contained no explosives. The package was destroyed and found to contain an assortment of items, including clothing. Source: http://www.azcentral.com/community/tempe/articles/2010/10/05/20101005tempe-suspicious-package-abrk.html

(Texas) **Part of Houston Ship Channel closed after barge collides with power line tower.** A 19-mile stretch of the Houston Ship Channel in Texas was closed to marine traffic October 3 after a barge slammed into a tower supporting a high-voltage electric transmission line, threatening to topple it into the channel. Coast Guard officials said a towing vessel named Safety Quest was pushing three barges loaded with scrap metal about 6 a.m. when it smashed into a Baytown power line, which remained upright only with the support of one of the barges. No injuries were reported, but the boat crew moved to another vessel and to safety. Officials closed the channel from mile marker 105 to 124 and said it could stay that way for up to 3 days. Centerpoint Energy officials said the power had been shut off to the line because crews had previously been working on a nearby tower. They said no customers had lost electricity following the crash. Coast Guard officials said the ship channel handles more than $320 million in cargo and crude oil daily, meaning the Port of Houston could lose nearly $1 billion if the waterway is closed for 3 days. Source: http://www.kvue.com/news/state/Part-of-Houston-Ship-Channel-closed-after-barge-collides-with-power-line-tower-104276529.html

Water and Dams

'Ecological catastrophe': Toxic sludge kills 3. The Hungarian government declared a state of emergency October 5 after a toxic sludge spill killed at least three people. The state of emergency affected Veszprem, Gyor-Moson-Sopron and Vas counties. Six people were missing October 5 and 120 injured in what officials said was an ecological disaster. The contaminated mud poured through Kolontar and two other villages October 4 after bursting out of an open containment pond at the nearby Ajkai Timfoldgyar Zrt plant, owned by MAL Zrt. The sludge, a waste product in aluminum production, contains heavy metals and is toxic if ingested. Many of the injured sustained burns as the sludge seeped through their clothes. Two of the injured were in life-threatening condition. An elderly woman, a young man and a 3-year-old child were killed in the flooding. Several hundred tons of

plaster were being poured into the Marcal river to bind the toxic sludge and prevent it from flowing, the National Disaster Management Directorate said. So far, about 35.3 million cubic feet of sludge has leaked from the reservoir and affected an estimated area of 15.4 square miles, the environmental affairs state secretary said. He said it was feared the sludge could reach the Raba and Danube rivers. Seven towns, including Kolontal, Devecser and Somlovasarhely, were affected near the Ajkai Timfoldgyar plant in the town of Ajka, 100 miles southwest of Budapest, the capital. Source: http://www.msnbc.msn.com/id/39513858/ns/world_news-europe/#

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**